Claims

WE CLAIM:

1. A method of associating a permission set with a code assembly based on evidence characterized by different levels of trust, the method comprising:

receiving at least a first condition and a first element of evidence, wherein the first condition is associated with the permission set and the level of trust associated with the first element of evidence is independent of other evidence and conditions;

receiving at least a second condition and a second element of evidence, wherein the second condition is associated with the permission set and the level of trust associated with the second element is dependent upon the first condition;

determining whether the first condition is satisfied by the first element of evidence;

determining whether the second condition is satisfied by the second element of evidence; and

associating the permission set with the code assembly, if both the first condition and the second condition are satisfied.

2. The method of claim 1 wherein the operation of receiving at least a first condition comprises:

receiving the first condition and the first element of evidence within a membership criterion.

3. The method of claim 1 wherein the operation of receiving at least a second condition

comprises:

receiving the second condition and the second element of evidence within a membership criterion.

4. The method of claim 1 wherein the operation of receiving at least a first condition comprises:

receiving the first condition in a membership criterion; and

reading the first element of evidence based on a reference included in the membership criterion.

5. The method of claim 1 wherein the operation of receiving at least a second condition comprises:

receiving the second condition in a membership criterion; and

receiving the second element of evidence based on a reference included in the membership criterion.

6. The method of claim 1 wherein the first condition applies the first element of evidence as implicitly trusted evidence used to validate the second element of evidence applied in the second condition.

7. The method of claim 1 wherein the second condition applies the second element of evidence as initially untrusted evidence.

8. The method of claim 1 further comprising:

generating a collection of code groups, each code group being associated with a membership criterion and a permission set, wherein the first condition and the second condition are received in the membership criterion associated with one of the code groups; and

determining whether the code assembly is a member of the code group, based on the membership criterion.

9. The method of claim 8 wherein the associating operation comprises:

associating the permission set of the code group with the code assembly, if the code assembly is determined to be a member of the code group.

10. The method of claim 1 further comprising:

receiving at least a third condition referencing a third element of evidence, wherein the level of trust associated with the third element is dependent upon the second condition; and

determining whether the third condition is satisfied by the third element of evidence, wherein the associating operation comprises associating the permission set with the code assembly, if the first condition, the second condition, and the third condition are satisfied.

11. A computer program product encoding a computer program for executing on a computer system a computer process for associating a permission set with a code assembly based on evidence characterized by different levels of trust, the computer process comprising:

generating a collection of code groups, each code group being associated with a membership criterion and a permission set;

receiving the membership criterion associated with one of the code groups, the membership criterion including at least a first condition and a second condition;

referencing a first element of evidence in the first condition, wherein the level of trust associated with the first element of evidence is independent of other evidence and conditions;

referencing a second element of evidence in the second condition, wherein the level of trust associated with the second element is dependent upon the first condition;

determining whether the first condition is satisfied by the first element of evidence;

determining whether the second condition is satisfied by the second element of evidence;

evaluating the first condition and the second condition using a logical operation to determine membership of the code assembly in the code group; and

associating the permission set with the code assembly, if the code assembly is determined to be a member of the code group.

12. The computer program product of claim 11 wherein the computer process further comprises:

receiving at least a third condition referencing a third element of evidence, wherein the level of trust associated with the third element is dependent upon the second condition; and

determining whether the third condition is satisfied by the third element of evidence, wherein the associating operation comprises associating the permission set with the code assembly, if the first condition, the second condition, and the third condition are satisfied.

13. A computer data signal embodied in a carrier wave by a computing system and encoding a computer program for executing a computer process associating a permission set with a code assembly based on evidence characterized by different levels of trust, the computer process comprising:

receiving at least a first condition referencing a first element of evidence, wherein the first condition is associated with the permission set and the level of trust associated with the first element of evidence is independent of other evidence and conditions;

receiving at least a second condition referencing a second element of evidence, wherein the second condition is associated with the permission set and the level of trust associated with the second element is dependent upon the first condition;

determining whether the first condition is satisfied by the first element of evidence;

determining whether the second condition is satisfied by the second element of evidence; and

associating the permission set with the code assembly, if both the first and second conditions are satisfied.

14. A computer program storage medium readable by a computer system and encoding a computer program for executing a computer process associating a permission set with a code assembly based on evidence characterized by different levels of trust, the computer process comprising:

receiving at least a first condition referencing a first element of evidence, wherein the first condition is associated with the permission set and the level of trust associated with the first element of evidence is independent of other evidence and conditions;

receiving at least a second condition referencing a second element of evidence, wherein the second condition is associated with the permission set and the level of trust associated with the second element is dependent upon the first condition;

determining whether the first condition is satisfied by the first element of evidence;

determining whether the second condition is satisfied by the second element of evidence; and

associating the permission set with the code assembly, if both the first and second conditions are satisfied.

15. A policy manager for associating a permission set with a code assembly based on evidence characterized by different levels of trust, the policy manager comprising:

a code collection generator generating a collection of code groups, each code group being associated with a membership criterion and a permission set;

a membership evaluator evaluating at least a first condition and a second condition associated with one of the code groups, the first condition referencing a first element of evidence in the first condition, wherein the level of trust associated with the first element of evidence is independent of other evidence and conditions; the second condition referencing the second element of evidence, wherein the level of trust associated with the second element is dependent upon the first condition; and

a permission set generator associating the permission set of the code group with the code assembly, if the code assembly is determined to be a member of the code group.

16. The policy manager of claim 15 wherein the membership evaluator further receives at least a third condition referencing a third element of evidence, wherein the third condition is associated with the permission set and the level of trust associated with the third element is dependent upon the second condition, and determines whether the third condition is satisfied by the third element of evidence, and

wherein the permission set generator associates the permission set with the code assembly, if the first condition, the second condition, and the third condition are satisfied.

17. A computer program product encoding a computer program for executing on a computer system a computer process for associating a permission set with a code assembly based on evidence characterized by different levels of trust, the computer process comprising:

receiving one or more first conditions, each first condition being associated with one or more first elements of evidence, wherein each first condition is associated with the permission set;

determining whether each first condition is satisfied by an associated first element of evidence;

generating an indication for each first condition that is satisfied;

receiving a second condition associated with the permission set;

determining whether the second condition is satisfied based on the indications; and

associating the permission set with the code assembly, if both the first condition and the second condition are satisfied.

18. The computer program product of claim 17 wherein the indication is associated with a first value associated with the first condition, and the operation of determining whether the second condition is satisfied comprises:

collecting the first value and additional values associated with other satisfied conditions to provide collected values;

summing the collected values to provide a sum; and

evaluating the sum against a threshold to determine whether the second condition is satisfied.

19. The computer program of claim 17 wherein at least one first element of evidence includes initially untrusted evidence.

20. The computer program of claim 17 wherein at least one indication includes initially untrusted evidence.

21. The computer program of claim 17 wherein the computer process further comprises:

generating an indication for each first condition that is not satisfied.